UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/457,914	12/10/1999	GERMANO CARONNI	06502.0289	8208

22852 7590 02/03/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	12

DATE MAILED: 02/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/457,914	CARONNI ET AL.	
	Examin r	Art Unit	
	LEYNNA T. HA	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the c rrespondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-45 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-45 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 11 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-45 have been examined and is rejected under 35 U.S.C. 102(e).

2. The Specification is objected.

3. Conclusion

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

1. Claims 1-45 are rejected under 35 U.S.C. 102(e) as being anticipated by Devine, et al. (US 6,606,708).

As per claim 1:

Devine, et al. teaches a method for providing communication access between a first process and a second process comprising the steps, executed in a data processing system, of:

appending security context information for the first process in a process table; **(col.9, lines 60-63 and col.13, lines 60-67)**

opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

transmitting a packet from the first process to the second process through the open socket including the security context information for the first process in the process table. **(col.13, lines 31-67)**

As per claim 2:

Devine discusses modifying a socket structure so as to accept the security context information. **(col.12, lines 34-37)**

As per claim 3:

Devine discloses receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

permitting use of the packet if the security context information is verified. **(c 1.9, lines 24-26)**

As per claim 4:

Devine discloses the method of verifying the security context information includes:

determining if the first and second process belong to a channel; and **(col.20, lines 53-63)**

accepting the transmitted packet when the first and second process belong to the channel. **(col.23, lines 7-16)**

As per claim 5:

Devine discloses the method of determining if the first and second process belong to a channel includes:

comparing the security context information in the received packet and security context information in another process table. **(col.27, line 43 thru col.28, line 5)**

As per claim 6:

Devine discloses the process table and the another process table are located on a single node. **(col.9, lines 60-66)**

As per claim 7:

Devine discloses the method of verifying the security context information includes:

determining whether the first and second process belong to two different linked channels; and **(c 1.20, lines 53-63 and c 1.22, lines 25-30)**

permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

As per claim 8:

Devine discloses the method of determining whether the first and second process belong to two different linked channels includes initiating a process that spawns two child processes that are connected by a shared-memory region in a memory. **(col.24, line 2 and col.26, lines 40-42)**

As per claim 9:

Devine discloses the method of permitting use of the packet includes decrypting the packet on a node and **(col.8, lines 27-28)** authenticating a sender associated with the first process on the node **(col.12, lines 34--37)**.

As per claim 10:

Devine discloses the method of appending security context information includes:

obtaining the security context information from a third process including a virtual address and a node identification; and **(col.9, lines 2-10 and col.23, lines 61-64)**

limiting each of the first, second and third processes to communicate with another process provided that the communication processes share the same node identification. **(col.22, lines 25-30 and col.26, lines 24-31)**

As p r claim 11:

Devine discloses modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit. **(col.13, lines 31-67)**

As per claim 12:

Devine teaches a method for placing processes executed in a node in security context, comprising of steps of:

sending a request from the node to a server to verify a username and a node identification associated with a process; **(col.14, lines 7-11)**

in response to the request, receiving security context information at the node from the server including a virtual address for the node; **(col.23, lines 61-64)**

initiating the process, and **(col.10, lines 38-41)**

appending the security context information and the node identification associated with the process in a process table. **(col.13, line 43 thru col.14, line 17)**

As per claim 13:

Devine discusses receiving security context information further includes receiving a key that corresponds to the node identification from the server. **(col.8, lines 52-55)**

As p r claim 14:

Devine discusses the method of claim 13, further comprising:

encrypting a packet transmitted by the process using the key;

(col.9, lines 6-13)

encapsulating the encrypted packet with a header that includes the node identification. **(col.13, lines 31-67) (col.9, lines 6-13)**

As per claim 15:

The method of claim 12, further comprising:

sending a second request from the node to the server to verify a username and node identification; **(col.10, lines 39-44)**

receiving additional security context information from the server, wherein the additional security context information includes a second virtual address for the node; **(col.23, lines 61-63)**

creating a second process; and **(col.24, lines 60-64)**

appending the security context information for the second process in the process table that is associated with the second process. **(col.13, line 43 thru col.14, line 17)**

As per claim 16:

Devine teaches a method for providing secure communications between a first process and a second process comprising the steps, executed in a data processing system, of:

obtaining a node identification and a virtual address; **(c 1.9, lines 2-10 and col.23, lines 61-64)**

including the node identification and the virtual address in a field corresponding to the first process in a process table; **(col.14, lines 7-11 and col.23, lines 61-63)**

transmitting a datagram that contains the node identification and the virtual address from the first process to a socket; and **(col.24, lines 60-64)**

receiving the datagram at the second process that contains the node identification and a second virtual address. **(col.14, lines 7-11 and col.23, lines 61-64)**

As per claim 17:

Devine teaches the method of claim 16, wherein obtaining a node identification and a virtual address further includes:

modifying a socket structure in the socket so that the socket structure accepts the node identification and the virtual address; and **(col.13, lines 31-67)**

modifying a process table so that the table includes a node identification field and a virtual address field. **(col.23, lines 26-31 and col.26, lines 24-31)**

As p r claim 18:

Devine teaches a system for providing communication access between a first process and second process, comprising:

means for appending security context information for the first process in a process table; **(col.9, lines 60-63 and col.13, lines 60-67)**

means for opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

means for transmitting a packet from the first process to the second process through the open socket including the security context information for the first process in the process table. **(col.13, lines 31-67)**

As per claim 19:

Devine discloses means for modifying a socket structure so as to accept the security context information. **(col.12, lines 34-37)**

As per claim 20:

Devine discloses means for receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

means for verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

means for permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

As per claim 21:

Devine discloses the means for verifying the security context information includes:

means for determining if the first and second process belong to a channel; and **(col.20, lines 53-63) (col.23, lines 7-16)**

means for accepting the transmitted packet when the first and second process belong to the channel. **(col.23, lines 7-16)**

As per claim 22:

Devine discloses the system of claim 21, wherein means for determining if the first and second process belong to a channel includes:

means for comparing the security context information in the received packet and security context information in another process table. **(col.27, line 43 thru col.28, line 5)**

As per claim 23:

Devine discloses the system of claim 22, wherein the process table and the another process table are located on a single node. **(col.9, lines 60-66)**

As per claim 24:

Devine discloses the system of claim 20, wherein means for verifying the security context information includes:

means for determining whether the first and second process belong to two different linked channels; and **(c 1.20, lin s 53-63 and c 1.22, lines 25-30)**

means for permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

As per claim 25:

Devine discloses a system of claim 24, wherein means for determining whether the first and second process belong to two different linked channels includes:

means for initiating a process that spawns two child processes that are connected by a shared-memory region in a memory. **(col.24, line 2 and col.26, lines 40-42)**

As per claim 26:

Devine discloses the system of claim 24, wherein means for permitting use of the packet includes:

means for decrypting the packet on a node; and **(col.12, lines 34--37)**.

means for authenticating a sender associated with the first process on the node. **(col.8, lines 27-28)**

As per claim 27:

Devine includes the system of claim 18, wherein means for appending security context information includes:

means for obtaining the security context information from a third process including a virtual address and a node identification; and

(col.9, lines 2-10 and col.23, lines 61-64)

means for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification. **(col.22, lines 25-30 and col.26, lines 24-31)**

As per claim 28:

Devine discusses the system of claim 18, further comprising:

means for modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit. **(col.13, lines 31-67)**

As per claim 29:

Devine teaches a system for placing a process executed in a node in a security context, comprising:

a server; and **(col.8, line 25)**

a sending node comprising:

a transmission module that transmit a request to the server to verify a username and a node identification **(col.12, lines 36-37)**, and receives security context information from the server in response to the request, wherein the security context information includes a virtual address for the sender node; **(col.23, lines 26-28)**

memory containing a process and an associated process table; and **(col.13, lines 60-67)**

an appending module that appends the received security context information and the node identification for the process in the process table. **(col.13, line 43 thru col.14, line 17)**

As per claim 30:

Devine discloses the system of claim 29, wherein the transmission module further receives a key that corresponds to the node identification from the server. **(col.8, lines 52-55)**

As per claim 31:

The system of claim 30, further comprising:

an encryption module that encrypts a packet transmitted by the process using the key; **(col.9, lines 6-13)**

an encapsulating module that encapsulates the encrypted packet with a header that includes the node identification. **(col.13, lines 31-67)**

As per claim 32:

The system of claim 29, further comprising:

a gateway that provides communication between the process and a second process executing in the node, and **(col.22, lines 21-22)**

wherein the transmission module further sends a second request to the server to verify a username and node identification **(col.10, lines 39-44)**, and receives additional security context information from the server **(col.23, lines 61-63)**, wherein the additional security context information includes a second virtual address for the node; **(col.24, lin s 60-64)**

appending the security context information for the second process in a process table that is associated with the second process. **(col.13, line 43 thru col.14, line 17)**

As per claim 33:

Devine teaches a system for providing secure communications between a first process, comprising:

means for obtaining a node identification and a virtual address; **(col.9, lines 2-10 and col.23, lines 61-64)**

means for including the node identification and the virtual address in a field corresponding to the first process in a process table; **(col.14, lines 7-11 and col.23, lines 61-63)**

means for transmitting a datagram that contains the node identification and the virtual address from the first process to a socket; and **(col.24, lines 60-64)**

means for receiving the datagram at the second process that contains the node identification and a second virtual address. **(col.14, lines 7-11 and col.23, lines 61-64)**

As per claim 34:

Devine discloses the system of claim 33, wherein means for obtaining a node identification and a virtual address further comprises:

means for modifying a socket structure in the socket so that the socket structure accepts the node identification and the virtual address; and

(c 1.13, lin s 31-67)

means for modifying a process table so that the table includes a node identification field and a virtual address field. **(col.23, lines 26-31 and col.26, lines 24-31)**

As per claim 35:

Devine discloses a computer readable medium for controlling a data processing system to perform a method for providing communication access between a first process and a second process, comprising:

an appending module for appending security context information for the first process in a process table; **(col.9, lines 60-63 and col.13, lines 60-67)**

an opening module for opening a socket between the first process and the second process; and **(col.8, lines 22-26)**

a transmitting module for transmitting a packet from the first process to the second process through the open socket including the security context information for the first process in the process table. **(col.13, lines 31-67)**

As per claim 36:

The computer readable medium of claim 35, further comprising a modifying module for modifying a socket structure so as to accept the security context information. **(col.12, lines 34-37)**

As per claim 37:

The computer readable medium for claim 35, further comprising:

a received module for receiving the packet at the second process through the socket; **(col.8, lines 33-35)**

a verifying module for verifying the security context information received in the packet; and **(col.11, line 41 thru col.12, line 12)**

a permitting module for permitting use of the packet if the security context information is verified. **(col.9, lines 24-26)**

As per claim 38:

The computer readable medium of claim 36, wherein the verifying module includes:

a determining module for determining if the first and second process belong to a channel; and **(col.20, lines 53-63)**

an accepting module for accepting the transmitted packet when the first and second process belong to the channel. **(col.23, lines 7-16)**

As per claim 39:

The computer readable medium of claim 38, wherein the determining module includes:

a comparing module that compares the security context information in the received packet and security context information in another process table. **(col.27, lin 43 thru col.28, line 5)**

As per claim 40:

The computer readable medium of claim 39, wherein the process table and the another process table are located on a single node. **(col.9, lines 60-66)**

As per claim 41:

The computer readable medium of claim 37, wherein the verifying module includes:

a determining module for determining whether the first and second process belong to two different linked channels; and **(col.20, lines 53-63 and col.22, lines 25-30)**

a permitting module for permitting use of the packet when the different channels are linked. **(col.23, lines 7-11)**

As per claim 42:

The computer readable medium of claim 41, wherein the determining module includes a initiating module that initiates a process that spawns two child processes that are connected by a shared-memory region in a memory. **(col.24, line 2 and col.26, lines 40-42)**

As per claim 43:

The computer readable medium of claim 41, wherein the permitting module includes:

a decrypting module for decrypting the packet on a node; and **(col.12, lin s 34--37)**.

an authenticating module for authenticating a sender associated with the first process on the node. **(col.8, lines 27-28)**

As per claim 44:

The computer readable medium of claim 35, wherein the appending module includes:

an obtaining module for obtaining the security context information from a third process including a virtual address and a node identification; and **(col.9, lines 2-10 and col.23, lines 61-64)**

a limiting module for limiting each of the first, second and third processes to communicate with another process provided that the communicating processes share the same node identification. **(col.22, lines 25-30 and col.26, lines 24-31)**

As per claim 45:

The computer readable medium of claim 35, further comprising:

a modifying module for modifying a network stack such that the network stack requires the security context information to be present in the socket structure to transmit. **(col.13, lines 31-67)**

Specification

2. ***The disclosure is objected to because of the following informalities:***

Pages 1-2 fails to provide the (12) US patent application numbers.

Appropriate correction is required.

Conclusion

For more details and information for the cited rejections above, please refer to Devine, et al. (US 6,606,708): Col.3, line 9...ET. Seq.

3. ***The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (703) 305-3853. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) ~~746-~~ 872 ~~7239~~ 9306

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5631.

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

LHa